I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Explotación de vulnerabilidad / Ejecución remota de comandos (RCE)
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Explotación Activa de Vulnerabilidad de Ejecución Remota de Código en Zimbra (CVE-2026-73570) - figura referencial

Se ha identificado una vulnerabilidad crítica de explotación activa en Zimbra Collaboration Suite (ZCS), catalogada como CVE-2026-73570. Esta falla permite a un atacante no autenticado ejecutar comandos de forma remota en servidores que tengan instalado el componente zimbra-snmp y las notificaciones Simple Network Management Protocol (SNMP) habilitadas, comprometiendo potencialmente la integridad y disponibilidad del sistema.

III. INTRODUCCIÓN

ZCS es una plataforma de software colaborativo (groupware) de código abierto que integra servicios de correo electrónico, calendarios compartidos, libretas de contactos, gestión de tareas y almacenamiento de archivos. Además, ofrece administración centralizada para gestionar cuentas, dominios y servidores mediante una consola web y una interfaz de línea de comandos, así como acceso desde clientes de escritorio y dispositivos móviles.

También incorpora un sistema de monitoreo basado en SNMP que permite supervisar el estado y funcionamiento de sus servidores y servicios. Para ello, utiliza el componente zimbra-snmp, que es opcional y puede instalarse en los servidores que forman parte de su implementación. Este componente emplea un conjunto de herramientas de Net-SNMP para recopilar información del sistema y SwatchDog para supervisar los registros de syslog y generar notificaciones SNMP ante determinados eventos o errores, que posteriormente pueden ser recibidos por una plataforma de monitoreo externa.

El equipo polaco de Respuesta a Emergencias Informáticas (CERT Polska) ha advertido que la vulnerabilidad CVE-2026-73570 está siendo explotada activamente. Esta falla de inyección de comandos permite a un atacante no autenticado ejecutar código de forma remota mediante la explotación del componente de monitoreo SNMP, cuando estas mismas notificaciones están habilitadas en el sistema objetivo.

IV. VECTOR DE ATAQUE

CVE-2026-73570, esta vulnerabilidad posee una severidad CRITICA con una puntuación CVSS: 3.1 de 8.9 tipo RED /AV: N/AC: L/PR: N/UI: N/S: U/C: H/I: H/A: H

La explotación de CVE-2026-73570 se da cuando el administrador instala el paquete opcional zimbra-snmp y además habilitó las notificaciones SNMP con el servicio Swatchdog en ejecución. Debido a una sanitización inadecuada de datos de entrada no fiables durante el procesamiento de notificaciones SNMP, un atacante no autenticado podría enviar solicitudes Simple Mail Transfer Protocol (SMTP) especialmente diseñadas que podrían dar lugar a la ejecución de comandos arbitrarios del sistema con los privilegios del usuario de Zimbra.

A partir de ahí, los atacantes pueden ejecutar comandos maliciosos, crear o modificar archivos, instalar Web Shells, robar datos de correo electrónico, establecer persistencia o utilizar el servidor comprometido para atacar otros sistemas dentro de una organización.

V. IMPACTO

Zimbra Collaboration Suite (ZCS) en versiones anteriores a 10.1.20, debido a la presencia de la vulnerabilidad de seguridad identificada como CVE-2026-73570.

VI. INDICADORES DE COMPROMISO

- Solicitudes SMTP anómalas o especialmente diseñadas dirigidas hacia servidores Zimbra.
- Actividad SMTP proveniente de fuentes externas desconocidas o sospechosas.
- Procesos o comandos inesperados ejecutados bajo el usuario Zimbra.
- Procesos secundarios no habituales generados por componentes de Zimbra.
- Archivos nuevos o modificados de forma inesperada en el servidor.
- Conexiones salientes no autorizadas desde servidores Zimbra.
- Modificaciones inesperadas en configuraciones de Zimbra o del sistema operativo.
- Creación de cuentas, tareas programadas o mecanismos de persistencia no autorizados.
- Actividad anómala asociada con el paquete zimbra-snmp.
- Evidencia de ejecución de comandos del sistema operativo coincidente temporalmente con solicitudes SMTP sospechosas.
- Claves SSH, cuentas u otros mecanismos de acceso creados sin autorización.

VII. RECOMENDACIONES:

- Actualizar Zimbra Collaboration a la versión 10.1.20 o una versión superior que incluya la corrección de seguridad correspondiente.
- Realizar un inventario de las plataformas Zimbra desplegadas en la infraestructura y comprobar la versión instalada en cada servidor.
- Comprobar la presencia del componente zimbra-snmp en los servidores Zimbra identificados.
- Validar la configuración de SNMP y determinar si las notificaciones SNMP se encuentran activas.
- En aquellos entornos donde SNMP no sea requerido para la operación, considerar su desactivación de acuerdo con las recomendaciones oficiales del fabricante.
- Analizar los registros de los servidores Zimbra, prestando especial atención a solicitudes o comportamientos que puedan resultar inusuales.
- Examinar el archivo /var/log/zimbra.log para identificar eventos inesperados relacionados con cambios en el estado de los servicios.

- Inspeccionar archivos creados o modificados recientemente bajo el usuario zimbra, dando prioridad a las siguientes ubicaciones: /opt/zimbra/jetty/webapps/, /opt/zimbra/jetty_base/webapps/ y /tmp/.
- Monitorear la ejecución de procesos asociados al usuario zimbra e investigar aquellos que no correspondan con el funcionamiento habitual del servicio.
- Analizar las conexiones de salida generadas por los servidores Zimbra, especialmente aquellas dirigidas hacia direcciones IP, dominios o infraestructura externa no reconocida.
- Verificar la existencia de mecanismos de persistencia, incluyendo archivos, procesos, cuentas de usuario o configuraciones creadas recientemente que puedan estar relacionados con una posible intrusión.
- Restringir la exposición directa a Internet de las interfaces administrativas y demás servicios de Zimbra que no requieran acceso público.
- Fortalecer el monitoreo y filtrado del tráfico SMTP, aplicando controles adicionales cuando las características de la infraestructura lo permitan.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

THE HACKER NEWS. (2026). *Attackers Exploit Zimbra SNMP Flaw for Unauthenticated Remote Code Execution.*https://thehackernews.com/2026/08/attackers-exploit-zimbra-snmp-flaw-for.html

HISPASEC. (2026). *CISA exige parchear un fallo de Zimbra que ya se explota para ejecutar comandos sin autenticación.*https://unaaldia.hispasec.com/cisa-exige-parchear-un-fallo-de-zimbra-que-ya-se-explota-para-ejecutar-comandos-sin-autenticacion/

BLEEPINGCOMPUTER. (2026). *Hackers breached over 270 Zimbra servers in ongoing attacks.*https://www.bleepingcomputer.com/news/security/hackers-breached-over-270-zimbra-servers-in-ongoing-attacks/

CYBERSECURITY NEWS. (2026). *Zimbra Collaboration Suite Vulnerability Actively Exploited in the Wild.*https://cybersecuritynews.com/zimbra-collaboration-suite-vulnerability-exploited/

CVE DETAILS. (2026). *CVE-2026-73570.*https://www.cvedetails.com/cve/CVE-2026-73570/